FT MONROE INFORMATION TECHNOLOGY (IT) NETWORK ACCEPTABLE USE POLICY

1. Understanding. I understand that I have the primary responsibility to safeguard the information contained in the Secret Internet Protocol Router Network (SIPRNET/army.smil.mil) and/or Non-secure Internet Protocol Router Network (NIPRNET)/army.mil) from unauthorized or inadvertent modification, disclosure, destruction, denial or service, and use.

2. Access. Access to this network is for official use and authorized purposes and as set forth in DOD Directives 5500.7-R, "Joint Ethics Regulation" or as further limited by this policy.

3. Revocability. Access to Army resources is a revocable privilege and is subject to content monitoring and security testing.

4. Classified information processing. SIPRNET is the primary classified Information System (IS) for the Fort Monroe Directorate of Information Management (DOIM). SIPRNET is a classified only system and approved to process SECRET collateral information as SECRET and with SECRET handling instructions.

The SIPRNET is authorized for SECRET level processing in accordance with accredited SIPRNET Connection Approval File Number D960148, Identification: CCSD7184. The classification boundary between SIPRNET and NIPRNET requires vigilance and attention by all users. The ultimate responsibility for ensuring the protection of information lies with the user. The release of TOP SECRET information through the SIPRNET is a security violation and will be investigated and handled as a security violation or as a criminal offense.

5. Unclassified information processing. NIPRNET is the primary unclassified information system for the Fort Monroe DOIM. NIPRNET is an unclassified system.

a. NIPRNET provides unclassified communication to external DOD and other United States Government organization. Primarily, this is done via electronic mail and Internet networking protocols such as web, ftp, and telnet.
b. NIPRNET is approved to process UNCLASSIFIED, SENSITIVE information in accordance with local automated information system security management policies. The Garrison DAA has accredited this network for processing this type of information.
c. The NIPRNET and the Internet, as viewed by the DOIM, are synonymous. E-mail and attachments are vulnerable to interception as they traverse the NIPRNET and Internet, as well as all inbound/outbound data, external threats (e.g. worms, denial of service, hacker) and internal threats.
d. CAC/PKI Use:
    1. Sending Digitally Signed E-Mails. As a general rule in the Army, a PKI digital signature should be used whenever E-mail is considered "Official Business" and contains sensitive information. The digital signature provides assurances that the integrity of the message has remained intact in transit, and provides for the non-repudiation of the message that the sender cannot later deny having originated the E-mail.
    2. Encrypted Emails. Encrypted mail should be the exception, and not the rule. It should only be used to send sensitive information, information protected by the Privacy Act of 1974, and Information protected under the Health Insurance Portability and Accountability Act (HIPPA).

6. Minimum-security rules and requirements. As a SIPRNET and/or NIPRNET system user, the following minimum security rules and requirement apply:

a. Personnel are not permitted access to SIPRNET or NIPRNET unless in complete compliance with the DOD, Army personnel security requirement for operating in a SECRET system-high environment.

b. I have completed the security awareness-training (e.g. Annual AT Awareness Training Level I or Computer Security for Users) at _____ (name the location) and provided proof of completion to(name of the recipient)_____. I will participate in all training programs as required user training as an annual requirement IAW AR25-2 (inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification, and non-standard threats such as social engineering) before receiving system access.

c. I will generate, store, and protect passwords or pass-phrases. Passwords will consist of at least 10 characters with 2 each of uppercase and lowercase letters, numbers, and special characters. I am the only authorized user of this account. (I will not use my user ID, common names, birthdays, phone numbers, military acronyms, call signs or dictionary words as passwords or pass-phrases.), IAW AR25-2, Chapter 4, Section IV, Para 4-12 passwords should be changed at least every 90 days.

d. I will use only authorized hardware and software. I will not install or use any personally owned hardware, software, shareware, or public domain software.

e. To protect the systems against viruses or spamming, I will use virus-checking procedures before uploading or accessing information from any system, diskette, attachment, compact disk, thumb storage device, or other storage media.

f. I will not attempt to access or process data exceeding the authorized IS classified level.

g. I will not alter, change, configure, or use operating system or programs, except as specifically authorized.

h. I will not introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code.

i. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the IS and will not disseminate it to anyone without a specific need to know.

j. I will not utilize Army- or – DOD – provided ISs for commercial financial gain or illegal activities.

k. Maintenance will be performed by the System Administrator (SA) only.

l. I will use screen locks and log off the workstation when departing the area.

m. I will immediately report any suspicious output, files, shortcuts, or system problems to the SA and /or the Information Assurance Security Officer (IASO) and cease all activities on the system. The Monroe Helpdesk should be contacted at 788-3055 or forward an email message to

helpdesk@monroe.army.mil for assistant and to report any classified spillage. The classified spillage will be reported to the Monroe Security Officer and Network Managers for action.

n. I will address any questions regarding policy, responsibilities, and duties to the DOIM SA and/or IASO.

o. I understand that each IS is the property of the Army and is provided to me for official and authorized uses. I further understand that each IS is subject to monitoring for security purposes and to ensure that use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the IS and may have only a limited expectation of privacy in personal data on the IS. I realized that I should not store data on the IS that I do not want others to see.

p. I understand that monitoring of SIPRNET and NIPRNET will be conducted for various purposes and information captured during monitoring may be used for possible adverse administrative, disciplinary or criminal actions. I understand that the following activities are prohibited uses of an Army IS:

1. Unethical use (e.g. Spam, profanity, sexual misconduct, gaming, extortion).
2. Entering and showing unauthorized sites (e.g. pornography, streaming videos, E-Bay, chat rooms).
3. Entering and showing unauthorized services (e.g. peer-to-peer, distributed computing).
4. Unacceptable use of e-mail include exploiting list servers or similar group broadcast systems for purposes beyond intended scope to widely distribute unsolicited e-mail; sending the same e-mail message repeatedly to interfere with recipient's use of e-mail; sending or broadcasting, e-mail messages of quotations, jokes, etc., to multiple addressees; sending or broadcasting unsubstantiated virus warnings from sources other than IAMs (e.g. mass mailing, hoaxes, auto-forwarding).
5. Any use that could cause congestion, delay, degradation or disruption of service to any government system or equipment is unacceptable use (e.g., video, sound or other large files, "push" technology on the internet and other continuous data streams).
6. To show what is deemed proprietary or not releasable (e.g. Use of keywords, phrases or data identification).

q. I understand that I may use an Army IS for limited personal communications by e-mail and brief internet searches provided they are before or after duty hours, break periods or lunch time, as long as they do not cause an adverse impact on the employee's official duties; are of reasonable duration, and causes no adverse reflection on DOD. Unacceptable use of services or policy violations may be a basis for disciplinary actions and denial of services for any user.

r. The authority for soliciting your social security number (SSN) is EO 939. The information below will be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting violations. Disclosure of this information is voluntary; however, failure to disclose information could result in denial of access to DOIM information systems.

7. **Acknowledgement**. I have read the above requirements regarding use of DOIM access systems. I understand my responsibilities regarding these systems and the information contained in them.

_____	_____
Directorate/Division/Branch	Date
_____	_____
Last Name, First, MI (print)	Rank/Grade and SSN (SSN: Last four digits)
_____	_____
Signature	Area Code and Phone Number